NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

USING WEB-BASED TECHNOLOGIES FOR NETWORK MANAGEMENT TOOLS

by

Arie Agami

June, 1997

Thesis Advisor: Suresh Sridhar
Associate Reader: Rex Buddenberg

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 1997	Master's Thesis

4. TITLE AND SUBTITLE USING WEB-BASED TECHNOLOGIES FOR NETWORK MANAGEMENT TOOLS

5. FUNDING NUMBERS

6. AUTHOR(S) Agami Arie

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/ MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(maximum 200 words)***

This thesis examines the recent developments in the application of Internet technology to the field of network management. Network management has become increasingly important and even critical for large organizations. The current solutions offered by the main network management vendors are very expensive, demand a lot of training, and have been implemented only in a centralized paradigm of management. New solutions to current network management tools problems may be found in the increasingly popular World Wide Web, Internet tools such as Java, and remote database access through the Internet, as well as an established user interface, which can be easily learned. The main advantage of this paradigm shift is the ability to provide any user in the organization with information about the network, as well as the ability to allow authorized users to handle a network problem from any machine or location. These new methods are examined with regards to the requirements of an ideal network management system, and the feasibility of implementing these methods, given current network configuration. A web-based network management prototype implementing a configuration management tool is described. New network management protocols are also investigated.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Web based Network Management	86
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFI- CATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

Approved for public release; distribution is unlimited

USING WEB-BASED TECHNOLOGIES FOR NETWORK MANAGEMENT TOOLS

Arie Agami
Major, Israel Air Force
B.Sc., Ben-Gurion University, Israel, 1989

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN
INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL
June 1997**

Author: _____
Arie Agami

Approved by: _____
Suresh Sridhar, Thesis Advisor

_____
Rex Buddenberg, Associate Reader

_____
Reuben Harris, Chairman
Department of Systems Management

ABSTRACT

This thesis examines the recent developments in the application of Internet technology to the field of network management. Network management has become increasingly important and even critical for large organizations. The current solutions offered by the main network management vendors are very expensive, demand a lot of training, and have been implemented only in a centralized paradigm of management. New solutions to current network management tools problems may be found in the increasingly popular World Wide Web, Internet tools such as Java, and remote database access through the Internet, as well as an established user interface, which can be easily learned. The main advantage of this paradigm shift is the ability to provide any user in the organization with information about the network, as well as the ability to allow authorized users to handle a network problem from any machine or location. These new methods are examined with regards to the requirements of an ideal network management system, and the feasibility of implementing these methods, given current network configuration. A web-based network management prototype implementing a configuration management tool is described. New network management protocols are also investigated.

TABLE OF CONTENTS

I. INTRODUCTION

Data Networks provide rapid and efficient access to large quantities of information. Although we are not always aware of it, we have come to rely heavily on data networks. Organizations depend on a complex, distributed computing environment to carry out their everyday business activities. Disruption of a network can be very critical to business, especially to military systems. Therefore, in order to keep data networks in good working order, network management tools are necessary. The average firm spends about 15% of its total information systems budget on network management [Ref. 1], and yet enterprise management solutions have not been delivered. Network management tools currently offered by the marketplace are very expensive (for both software and hardware) and require a lot of experience and knowledge. The complexity of managing a network-based enterprise should be addressed with a set of tools that can provide the infrastructure for network management solutions.

A paradigm shift in the concept of managing enterprise networks is investigated in this thesis. Vendors are looking for ways to develop a set of network management tools that are based on Internet technology. The cost and complexity of current network management systems can be addressed with simple but powerful web-based tools that are accessible from any platform.

Since the main network management protocol used currently is SNMP, most web-based ideas and solutions either suggest extensions to SNMP so that it can be invoked using HTTP, or implement SNMP functionality using Java classes and applets. These concepts and methods are explored in the thesis.

This thesis is organized as follows: Chapter II provides an overview of network management disciplines. Chapter III summarizes the main characteristics of, and the evaluation criteria for network management systems. Chapter IV focuses on web-based network management solutions. Chapter V describes a web-based network management prototype with a configuration management tool built for system management lab staff. Appendix A includes a user manual, which can be also accessed through the system on-line help. Appendix B includes a developer manual for maintenance and future changes.

II. NETWORK MANAGEMENT ISSUES

A. OVERVIEW OF NETWORK MANAGEMENT

1. Network Management Functional Areas

The concept of network management was motivated by the need to free network managers from performing routine maintenance tasks. It is more cost-effective if the system is self-regulating and, in the process, performs routine tasks for the network engineer or network manager.

Another motivating factor in the network management is the need for reliable end-to-end service, so that the network members can share information freely.

Network management is defined as "the process of controlling, monitoring and running the network in such a way as to insure its proper operation" [Ref.10]. The International Organization for Standards (OSI) - the network management forum defined five functional areas that should be included in a network management system:

- Fault management
- Configuration management
- Security management
- Performance management
- Accounting management

2. Fault Management

Fault management is the process of locating problems or faults in the data network. It discovers, isolates, and (if possible) solves the problem. This is a fundamental concept of network management, and it increases network reliability by allowing the network manager the ability to quickly detect problems and initiate recovery procedures. [Ref. 2]

Gathering information is the first step in identifying the fault. Two methods can be used: logging critical network events or occasionally polling network devices. There is a trade-off between the update time of the network status and the bandwidth that will be consumed. Relying solely on critical network events may not always yield the up-to-date status of every network device. On the other hand, occasionally polling network devices may increase overhead communication and bandwidth consumption. The following is an example of a bandwidth consumption cost:

> A network has 30 devices. The Up-to-date requirement is one minute, and the message size for polling is 100 bytes (each side). For each polling interval (2*100 byte * 30 devices* 8 bit/word) = 48,000 bits are needed. Polling over an hour is (48000 bits * 60 sec* 60 polling) = ~ 173 Mbit of bandwidth for polling. [Ref. 2, page 24]

A decision should be made about which faults the system manages. Not all faults will have the same priorities. Sometimes there are too many faults to manage. By identifying the most manageable faults the amount of useless information can be reduced. The determination of which faults to manage should be made as follows: [Ref. 2]

- The scope of control (which defines the amount of information to obtain from the network devices); for example, the central administrator handles the X.25

switch, IP router and bridges of WAN network, while the local administrator manages the faults of their particular devices and hosts.

- The size of the network: In a large data network only the critical events of the most important hosts and network devices should be managed.

The process of isolating the cause of the fault and correcting the fault if possible, depends on the tools that implement these functions. The method used to report the fault, and the impact it can have on other parts of the network is also important when choosing these tools.

3. Configuration Management

Configuration management is the process of keeping in touch with all the devices of a given network. This includes managing the inventory (e.g., hardware and software) and the topology of the devices. Keeping track of the network devices requires: [Ref. 2]

- Gathering data about the current network information.
- Modifying the network configuration based on the data that was gathered.
- Storing data and producing reports based on the data.

Configuration management has some benefits:

- Helping the network manager to compare the running configuration with that stored in the system.
- Providing (if designed to) an up-to-date inventory of network components.

The bandwidth consumption used when implementing an automatic configuration management, as well as the configuration for user/process priorities, should be carefully considered when selecting the implementation method.

4. Security Management

Security Management is concerned with providing services, reporting functions that support the implementation of the organization's security policies, and protecting network resources and user's information. Network security management should be an integral part of a network design. Security management includes four steps: [Ref. 2]

- Identifying sensitive information, i.e., which hosts on the network have sensitive information.
- Finding the access points to sensitive information: remote login, file transfer, e-mail, remote execution, and the network management system itself.
- Securing the access points: encryption on the data link level, packet filters to secure traffic flow, which is accomplishing packet filtering based upon network or media access control. Host authentication allows access to a service based on a source host identifier (i.e., the network address). User authentication identifies the user before allowing him an access. Key authentication maintains a key server to accomplish both host and user authentication.
- Maintaining the secure access points.
- Auditing to detect system breakers.

5. Performance Management

To ensure that the network has the capacity to accommodate users' needs, the network manager needs performance management tools. These tools support the performance of the network software, hardware, and media. Performance can be measured by, for example, overall throughput, percentage utilization, error rates and response time. Performance management includes the following steps: [Ref. 2]

- Collect data on current utilization of network devices and links.

- Analyze relevant data, i.e., represent the analyzed data on a graph to assist the manager with the utilization of the network, error rates, and processor usage. These can be used to plan future network capacity.

- Set utilization thresholds. Utilization thresholds are set in order to warn the user when the network reaches certain error rates.

- Simulate the network. Network simulation is a very important tool to measure network efficiency and performance. The problem is the complexity involved in measuring performance and, therefore, the cost of these tools.

In order to measure the level of service, three values are determined: [Ref. 2]

- Total response time, the amount of time it takes the network to process data from end to end.

- Rejection rate - the percentage of time the network cannot transfer information.

- Availability - the ratio between the "up time" and "total time" of the system.

6. Accounting Management

Accounting management tools help the network manager to track the network utilization both by individual and group users, and to set usage quotas, using metrics, and billing users for their use of the network. Accounting management is a process of gathering network statistics. This can help the network manager make decisions regarding the allocation of network resources. The motivation for network accounting are: [Ref. 1]

- To prevent one user or a group of users from abusing access privileges and loading down the network at the expense of others.

- To assist users to make more efficient use of the network.

- To provide data for future growth projection and planning.

- To provide accurate data for billing purposes.

To handle accounting management, a network inventory must be maintained. Some network management systems use an inventory database in conjunction with their fault management system [Ref. 2].

B. THE REQUIREMENTS OF NETWORK MANAGEMENT TOOLS

1. Fault Management Tools

An ideal fault management system would detect, isolate, and fix a fault prior to it becoming a major problem. This process should be transparent to the user. Fang and Leinwand [Ref. 2], suggest three classifications for fault management tools: (1) simple tool that would warn the user of the existence of a problem, but would not indicate its cause, (2) more complex tool that would take advantage of the network device capability to report network events. This capability can be used to investigate the devices for further information once they have sent a critical event message. Furthermore, the management tool can query the devices to logically determine the origin, cause, and level of the problem. An advanced fault management tool will also try to correct the problem, for example, when two systems cannot communicate via e-mail. After testing the path between them, if it seems like there is no sign of a fault, the management tool tests each device on the path (using a management protocol) and finds that the problem is on the hub's connection. An advanced tool can solve the problem by shifting a port on the hub (assuming the hub software allows it).

2. Configuration Management Tools

A configuration management tool should provide two main facilities: First, the network information (e.g., addresses, serial numbers, and physical locations) about all the managed and unmanaged objects in the network, modifying their configurations when necessary. The second facility contains information to control and retrieve on each of these objects. This can be implemented by inventory management, which involves storing

the profile of each object in the network, and by topology management, which shows how the objects are interconnected. The user of this tool should not be intimidated by the complexity of the system. An ideal configuration management tool would allow the manager to visualize the network from end to end, and provide the capability to investigate further to each successive layer and individual component. Additionally, the tool should allow the manager to configure the operating attributes of certain components. Fang and Leinwand[Ref.2], suggested an advanced tool that will automatically gather and store information from all network devices. This can be further improved by adding a comparison tool so the information gathered can be compared to the current information.

> Example: In typical setup of a WAN, ...many cluster controllers exist at a single site with WAN links back to the central site, which houses a mainframe computer. Suppose that, on one controller, the response time from each terminal was slower than that from terminals on the other controllers. The configuration management tool, upon evaluating this setup, would recognize that the speed setting on that cluster controller was set to transmit at 4800 BPS, while the front-end processor at the other side of the link was set to receive at a maximum of 9600 BPS, resulting in a maximum speed of 4800 BPS. In contrast, all the other cluster controllers at the same site, talking to the same front-end processor, were set up to 9600 BPS communications on both sides. The tool would conclude that the discrepancy in bit rate of the controller in question caused its slower response time. As a final step in the evaluation, the tool would use the database to determine the actual speed of the wide area link.[Ref. 2 p. 50]

3. Security Management Tools

A security management tool should provide three main features: [Ref.11]

- Authentication, that is allowing the receiving party to verify that the message is from the alleged source.

- Privacy, which protects transmitted data from eavesdropping.

- An access control mechanism, which can be used to restrict access by a manager to certain users or network addresses.

An advanced security tool would be able to monitor the access points to sensitive information. Once a successful access is monitored (for example, too many unsuccessful remote login attempts), an alert would be sent to the network manager and/or to the log file. The tool would also examine the type of security one intends to install on a computer or device and alert the user to a possible violation of such installations. [Ref. 2]

4. Performance Management Tools

A performance management tool should provide the following features: [Ref. 10]

- The ability to look at a frozen moment in time or a snapshot of network performance. This should help in finding network bottlenecks, devices memory utilization, error rates, and current bit rate.

- The ability to gather statistics over a period of time to evaluate the performance of certain network components in several areas, including whether they need to be upgraded, whether they are performing as expected, or if there is a need for expansion? The tool may automatically enable a backup circuit in case a threshold is reached. The "cost" of examining the historical data capabilities is the amount of storage the system has to have and manage.

- The ability to predict response time, rejection rates, and availability are very important. These capabilities are based on sufficient input and can be very useful when building a new network.

5. Accounting Management Tools

A good accounting management tool should be able to generate periodic reports on the usage of the network These reports can be very specific (e.g., all the users that have more than three unsuccessful logins) or more general in nature. Accounting management should also provide the ability to determine whether the network bandwidth is being utilized effectively. It should be able to forecast the need for network resources, and help users predict their network billing costs. Finally, an advanced tool should be able to determine whether a network trend will cause a quota to be reached. Once that happens, the network manager should select the resource or change the quota. [Ref. 2]

C. NETWORK MANAGEMENT PROTOCOLS

The purpose of Network management protocols is to provide a means of obtaining information from, or give instruction to network devices so that it will support the network management controlling and monitoring functions. There are two main network management protocols: the Simple Network Management Protocol (SNMP) and the Common Management Information Services/Protocol (CMIS/CMIP). Both protocols provide the tools needed to gain management information from the network, and both conform to the OSI seven-layer reference model. Both protocols provide the tools for investigating the network, but do not deal with the interface for the network manager.

The SNMP model includes four key elements: management station, management agent, management information base (MIB), and a network management protocol. The management system is usually a stand-alone system that usually provides the interface for the network manager. The management agent is resident in the network components that should be managed, such as, hosts, hubs, and routers. The agent responds to requests for information and actions from the management station. It may also asynchronously provide the management station with other important information. [Ref. 11]

SNMP exchanges network information through messages or Protocol Data Units (PDUs). A message can be seen as an object that contains variables with both titles and values [Ref. 1]. A collection of objects is referred to as the MIB, which functions as a collection of access points at the agent for the management station. There are five types of PDUs that SNMP employs to monitor a network: two deal with reading terminal data, two deal with setting terminal data, and one is the trap that is used for monitoring network events such as terminal start-ups or shut-downs. Figure 2-1 [Ref. 11], describes the protocol context of SNMP:

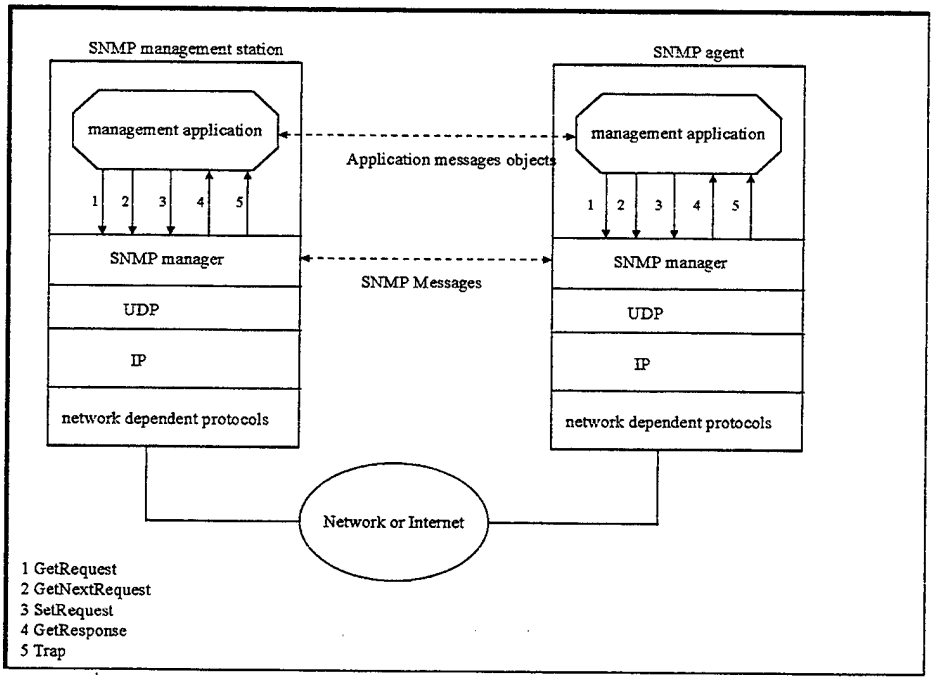

Figure 2-1. SNMP architecture.

SNMP operates as an application-level protocol using the TCP/IP protocol suite. In particular, it operates over the user datagram protocol (UDP). Since UDP is a connectionless protocol, SNMP is itself connectionless, which means that each exchange is a separate transaction between a management station and an agent [Ref.11]. This concept saves the overhead added by TCP for the "cost" of a reliable connection.

The main advantage of SNMP is its simple design; hence, it is easy to implement it in large networks. Furthermore, its simple design makes it easy for a user to program variables. SNMP is in a very wide use. Almost all major vendors of internetwork components, such as bridges and routers, design their products to support SNMP. The two main disadvantages of SNMP are the lack of manager-to-manger communication and the lack of security [Ref. 3]. The SNMPv2 has added some security mechanisms that help to face the largest security problems: privacy of data, authentication, and access control.

However, it has not received widespread acceptance, because developers found the security facility for SNMPv2 too complex [Ref. 1].

The CMIP is a larger and more detailed network protocol. Its basic design is similar to SNMP. CMIP has built-in security management devices that support authorization, access control, and security logs. The main disadvantages of CMIP are its complexity and the system resources it requires. Only a few very skilled programmers would be able to use the protocol variables. Furthermore, the system resources that CMIP uses are greater than SNMP-based system resources by a factor of ten to one.

III. ENTERPRISE NETWORK MANAGEMENT SYSTEMS

A. TYPICAL CHARACTERISTICS OF COMMERCIAL NETWORK MANAGEMENT SYSTEMS (NMS)

Commercially developed NMSs typically:

- Use the IP-based SNMP protocol to monitor many types of network elements (e.g., routers, bridges, and hubs) from a number of vendors.
- Are able to monitor large numbers of devices so that they can provide enterprise-wide monitoring.
- Can collect, archive, retrieve, and display information about the devices being monitored.
- Provide a platform on which third-party applications for the monitoring of specific devices can be run.
- Allow an operator to use graphical tools to make ad hoc inquiries about the state of the devices on the network.
- Run under UNIX or Windows NT operating systems, because SNMP is based on the TCP/IP protocol suite (an SNMP agent must have an IP address).
- Can be extended to provide services with locally developed systems.

B. REQUIRED FEATURES AND EVALUATION CRITERIA FOR ENTERPRISE NETWORK MANAGEMENT SYSTEMS

Different Network Management Systems (NMSs), should be evaluated according to a given list of features and evaluation criteria. Two different teams from the University of Michigan and Air Education and Training Command evaluated NMSs. The following is a brief list of features and criteria they used to evaluate NMSs [Ref. 4 & Ref. 8]. These features can be used as an excellent skeleton for evaluating a network management systems.

1. Required Features

a. Monitoring Features

- Ability to monitor computer system resources, and process via SNMP.
- Auto discovery.
- Support for specific vendors routers (e.g., Cisco, Cabletron).
- Dependency support.
- Network Operating system support for different networks (e.g., AppleTalk, NetWare).
- NMS application to support generic Remote monitoring (RMON) devices.
- Support for multiple distributed servers.

b. Administration Features

- Autonomous administration by departments and groups.
- Clear design paradigm.
- Flexible, comprehensive security.
- Notification flexibility.
- Built-in, but customizable database for customer.
- Availability of third-party application.
- Trouble ticket interface.
- Uses commercial relational database system for data storage.

c. Usability Features

- API for program access to real-time data.
- Flexible generation of reports from historical data.
- Flexible, user-friendly display of information.
- Powerful, non-programmed tools.
- Training and documentation.
- Vendor product support.

2. Evaluation Criteria

a. Automatic Topology Discovery and Configuration

A network management system should be able to discover the nodes and the configuration of a network. A user should have the capability to:

- Run discovery at any pre-determined time.
- Discover a specific network, a group of devices in the specified range of addresses, or a specific device.
- Alter the arrangement of discovered entities in a given view, and also group entities into different hierarchical levels.
- Add new entities manually and relate them to the discovered ones.

b. Notification Methods

An NMS should provide flexible notification methods. It should either support directly, or support via programming interface, notification via electronic mail, touch-tone pagers, text pagers, sound, and alarm screens displaying lists of alarms, preferably by severity.

c. Intelligent Monitoring

An NMS should be able to analyze the network and the inherent dependencies, and to report only known problems. A user should be able to add intelligence to an NMS to assist in monitoring. For example, a user might want to page

someone if a disk partition on a mail server is at more than 90% capacity for more than 30 minutes. Or, the user also might want to send e-mail to a responsible person if one of the servers fails and page someone if more than one fails.

d. Degree of Control

An NMS should provide the user with good control of when, where and what needs to be monitored. The areas of control include which devices are monitored, which MIB variables need to be monitored, the importance of each device, which alerts are critical, and the action to be taken on each alarm. The NMS should be flexible in terms of how it decides that a service has failed, and which steps should be taken. The polling interval of entities should be user-modifiable. The user should also be able to turn on or off the polling of an entity for a specified time interval. Polling should automatically revert to the previous state after the time interval has elapsed.

e. Flexibility and Customization

A user should be able to customize the NMS to specific operating needs. For example, it should be possible to add a new menu item, or to execute a custom-built program.

f. Multi-vendor Integration

An NMS should be capable of managing networking entities from different vendors, both SNMP and non-SNMP. Entities include networking devices, such as hubs, routers; Software servers, such as name-servers, and file-servers; telecommunication switches and other voice equipment, and computer workstations. In addition, an NMS

should be able to serve as a platform for running third-party application software packages, which support specialized monitoring of proprietary products.

g. Access Control

Flexible access control is needed to allow an administrator to determine the access control a user is permitted. A user might need read/write access to one department's network, but not access to another. Within a network itself, different users might need to have different access rights for the network's devices.

h. Architectural Issues

Some architectural issues should be considered. These include: a client-server approach, a multi-threaded server, the support of concurrent clients, the upper limit (if any) on the number of clients supported, if so is this limit placed by the server or is it dependent upon the hardware resources available? The suitability of the NMS product to a large and complex environment, the hardware platforms that the NMS can be run on, the kind of database that is used, the distribution capability the NMS has.

i. User Friendliness and Customization

An NMS should facilitate easy navigation through the system, present information in an organized and concise manner, and permit users to customize their environment, (e.g., by adding menu options, short-cuts, and script buttons). It should also provide support for a MIB browser so that a user can see which MIB objects are supported for an entity, and be able to view and set desired MIB variables. The user

should be able to control which information appears in reports produced by the NMS, and the formats used.

j. Programming Interfaces

An NMS should provide APIs, which permit easy and flexible extensions to be made to the NMS, such that programs can access all information stored in the NMS and provide custom information to it. An NMS, should also provide an application development environment that can run on a system other than the production system.

C. CHARACTERISTICS SUMMARY OF MAJOR ENTERPRISE NETWORK MANAGEMENT SYSTEMS

A report prepared by the University of Michigan Information Technology Division was written as part of an evaluation of a high-end Network management system [Ref. 4]. Another evaluation of NMSs was done by the U.S. Air Education and Training Command [Ref. 8]. The following chapter briefly explains the main characteristics of major NMSs from the evaluation reports.

1. Cabletron SPECTRUM

Cabletron SPECTRUM is an extensible and intelligent Network Management System (NMS) that utilizes an object-oriented, client-server architecture. SPECTRUM is built around an artificial intelligence engine, called the Inductive Modeling Technology, which, together with its object-oriented design, permits SPECTRUM to understand dependencies. SPECTRUM provides gateway support for Novell NetWare and Banyan VINES. Native protocol support (e.g., AppleTalk and IPX) could be added to

SPECTRUM by utilizing their External Protocol API, but it would require significant development. Spectrum characteristics include:

- Two methods of device polling: automatic (server initiated) and manual (operator initiated). The system administrator can specify which devices are to be polled and at which intervals, and which MIB variables are to be collected and logged for report generation. A difference between SPECTRUM, HP OpenView, and IBM NetView/6000 is that no redundant monitoring of devices occurs when multiple clients are monitoring the same device on different maps.

- Notification capabilities include an alarm screen (displaying a list of alarms by severity), sound, electronic mail, and pagers.

- SPECTRUM's auto discovery is quite flexible but is slower than other products. It permits one to discover selected sub-nets, selected IP address ranges, routers, and devices belonging to specific protocols.

- Administration Features: In SPECTRUM, network administrators can control the information that individual operators view on their console screens, thereby limiting access according to the responsibilities of each part of an organization. Local administrators can control access within their domains. The SPECTRUM MIB browser, called attribute walk, is complicated and awkward, requiring the user to specify instance IDs.

- Usability features: Through the SPECTRUM graphical user interface, users can customize their working environment, and create navigational short-cuts.

SPECTRUM provides the ability to view and control data in the server database from both its X-Windows interface, and as a command line interface.

Summary: SPECTRUM is a very powerful and flexible Network Management System. It provides some unique functions, such as the ability to determine dependencies and suppress erroneous alarms. SPECTRUM is a flexible system, and therefore has some complexity. Training is very important; without it, a user would have difficulty. Initial deployment of the product may also take longer because of its complexity. SPECTRUM has a limited number of third-party applications available.

2. Hewlett-Packard OpenView

HP OpenView is arguably the first comprehensive, off-the-shelf Network Management System (NMS) to gain wide market use. Although it is promoted as an enterprise-wide NMS, it really doesn't provide the same functionality provided by management systems specifically tailored for AppleTalk, NetWare, SNA, DECnet, X.25, Telecomm switches, and other non-SNMP devices. Nevertheless, HP has made great strides in improving OpenView from a development system product primarily for third-party application builders to an off-the-shelf product that end users can install and use fairly easily on their own. Its strongest attribute is its wide acceptance among third-party applications developers. IBM has enhanced and extended OpenView in their NetView/6000 product, which makes it well worth considering as an alternative to OpenView.

- Like NetView/6000, OpenView fails to perform any dependency heuristics before coloring a node or link red. The system characteristic of sending many

alerts as a result of a single router makes it seem as if the architecture does not have the knowledge of the overall environment outage.

- OpenView uses a commercial, relational database system. This makes it fairly easy for external applications to obtain information collected by OpenView, as well as to make SQL searches of the data easy. However, third-party applications are each responsible for storing their own information, which prohibits the sharing of such data.

- Like NetView/6000, OpenView redundantly monitors devices that are configured to be part of more than one network map.

- Administration Features: A major benefit of OpenView is the existence of many third party applications, more than are available for any other platform.

- The OpenView MIB browser, while better than Spectrum's attribute walk, is barely adequate. More precisely, problem-solving tools are required to deal with classes of problems and symptoms.

- Usability features: The user interface appears to be clean and fairly flexible, but it is more awkward to navigate than NetView/6000. The simple, easy-to-use Motif Graphic User Interface (GUI) provides status information and a topological view that most modern NMSs offer. A problem, however, is that all interactions with this package must be done through the X-Windows interface. There are no text-based alert screens, and it would be difficult to

build one using the supplied APIs. This restriction would make it difficult for on-call maintenance personnel to access information on a dial-up basis.

Summary: HPOpenView is an expensive, yet barely adequate NMS. It provides the base-level functionality required. Its strongest attribute is its wide acceptance among third-party applications developers. IBM has enhanced and extended OpenView in their NetView/6000 product which makes it well worth considering as an alternative to OpenView. In March 1996, HP unveiled the Tornado 2 release of HPOpenView, which offers expanded distributed management capabilities. This version lets managers use multiple UNIX workstations to gather information about networks of 10,000 nodes or more. It also includes a new management tool that enables users to handle some management tasks locally without giving up the ability to pass management information to an enterprise management platform in the central network-control center. [Ref. 5]

3. IBM NetView/6000

IBM NetView/6000 is a comprehensive Network Management System (NMS). It can be used by end users as an off-the-shelf, plug-and-play NMS system as well as a development platform for new network management applications. IBM licensed HP OpenView 3.1 to be used as the original base for NetView/6000. Subsequently, IBM has extended it considerably and integrated it with other software to create the NetView/6000 product family, which IBM has licensed to DEC. Although it is promoted as an enterprise-wide NMS, like all the products considered here, NetView/6000really doesn't provide the same functionality provided by management systems specifically tailored for AppleTalk,

NetWare, SNA, DECnet, X.25, Telecomm switches, and other non-SNMP devices. NetView/6000 characteristics include:

- Monitoring Features: Like as HPOpenView, NetView/6000 fails to perform any dependency heuristics before coloring a node or link red. The architecture seems to be geared towards managing discrete entities with no knowledge of the overall environment.

- NetView/6000 uses a commercial, relational database system and have the same features of HPOpenView.

- Compared to OpenView, NetView/6000 has a much ability to filter and correlate information, and to use thresholds to reduce the number of SNMP alerts which are treated as actual alarms. As with all the NMSs evaluated, alarms can invoke UNIX scripts or third-party programs.

- Like OpenView, NetView/6000 redundantly monitors devices that are configured to be part of more than one network map. IBM makes a product called Systems Monitor/6000 that is a remote UNIX systems monitoring agent with about 600 MIB variables for AIX and HP/USX. This software also uses SNMP polls of devices on a local LAN and handles traps. It provides all this information to one or more NetView/6000 systems.

- IBM has a proxy agent for OS/2 Intel platforms which can monitor local devices and communicate via SNMP to a NetView/6000 utility. IBM claims

that the NetView/6000 utility is also capable of understanding and displaying maps of a Novell NetWare network.

- Administration Features: One of the biggest benefits of NetView/6000 is the existence of many third party applications.

- IBM has improved substantially the installation procedures inherited from OpenView, making it the easiest to install of the five products they evaluated.

- Usability Features: The NetView/6000 user interface appears to be clean and fairly flexible, and is easier to navigate than HPOpenView's interface. The simple, easy-to-use Motif GUI provides status information and a topological view that most NMSs offer. IBM has added an Event Card display which shows the most recent events in the form of index cards in a separate window.

Summary: IBM has made many improvements to HP OpenView, providing a much more complete network management system in their NetView/6000 product suite. The price for NetView/6000 is lower than the price of OpenView, yet NetView/6000 offers more features and flexibility. Nevertheless, some of the limitations of NetView/6000 are troubling. The lack of dependency pruning would make it difficult to implement automated management under this package. However, there are some filtering/correlation software enhancements that prune some alerts. The development environment is included with NetView/6000, so development and integration are readily available.

IV. WEB-BASED MANAGEMENT

A. THE MOTIVATION FOR WEB-BASED ENTERPRISE MANAGEMENT SYSTEMS

Trying to describe the skills of a large network manager can be simple: keep your organization network up and running 24 hours a day, seven days a week, preferably at peak performance. In order to handle big networks that span countries and include everything from IBM mainframes to laptops, and from multi-protocol routers to T1 multiplexers, network managers are using what have now become known as enterprise management systems. In today's client/server multi-vendor environment, the centralized method of control is applied to SNMP-based enterprise management systems. The network manager might divide the enterprise into multiple management domains that will be connected to a single, central platform, which then collects filtered data to create a high-level view of the entire enterprise [Ref. 5]. Another method is to build a hierarchical management structure where management stations are positioned in each level to gather and provide network management information.

How will network managers and others in their organizations employ Web browsers to help them perform their jobs better, faster, and more cost effectively? Using Web technology, the user can add, access, and navigate links in textual and multimedia information. Relationship management [Ref. 12] supported by Web techniques is suggested for managing information by creating, storing, maintaining, retrieving, filtering, customizing, presenting, connecting, and navigating relationships. Importing this idea into

network management can provide access to network management information. Using the relationships between the elements of different networks elements results in new ways to:

- View/retrieve the network's elements status
- Navigate among them
- Discover additional relationships
- Target information displays to individuals users and their tasks.

The World Wide Web (WWW) infrastructure can serve as an interface for the network manager and the organization users of the network to gain a clear picture of the network, as well as the relationships of and information about the network elements.

B. METHODS AND CONCEPTS IN WEB-BASED MANAGEMENT TOOLS

1. General Concepts and Methods in Web-Based Management

There are three fundamental applications where Web-based tools can provide a significant benefit: individual device configuration and management, browser access to sophisticated management applications, and corporate information systems access to the network status data. [Ref. 9]

(1) Web-based configuration and management of individual devices: This capability is aimed at managers and individual users of small networks who may not have their own network management system. These users want to configure and monitor the devices in their networks as easily as possible, and perhaps even gain some remote device management capabilities. For example, many SNMP-based tools use an ASCII interface to

ping network devices or to acquire SNMP data. What these users need are device configuration tools using a Web browser. This is accomplished by providing the equipment to be configured with an agent that includes a native HTML interface. The manager then enters basic configuration parameters for each device by completing a simple online electronic form. Remote monitoring of simple device statistics is also possible via the browser, using tabular and graphical displays of basic device information and performance. As in SNMP protocol, this concept is based on the assumption that the monitored device has an IP address.

(2) Web-based access from any desktop to advanced network-wide management capabilities: This application is targeted at enterprise network support staffs, who currently use network management solutions. Their goal is to monitor the network, understand potential faults and alarms, and provide their users with continuous network availability. Network management solutions, working in conjunction with popular platforms like HPOpenView, provide the foundation for these networks. Building on this foundation, Web browsers provide a number of low-cost options for easily accessing important information. For example, a staff member, out on the floor trouble-shooting the network, may need to access an application. Through a Web browser running on any PC or laptop in the organization, the user could access the necessary application and continue the trouble shooting process, regardless of location.

(3) Another method is Web reporting of network status information for browsing by information system management and others via the organization's intranet. Users of this application are information systems group managers who do not necessarily operate the network, nor get involved in extremely technical detail. Instead, their goal is to quickly

obtain information about the state of the network, about trends over time, and notification of any potential hot spots. The Web is an excellent tool for distributing this type of information. Various people within an organization have different needs for different types of information. Members of a finance group for instance, may need usage accounting information, while database users may need to determine system status, or submit an online trouble ticket and follow it through to resolution. The corporate intranet offers a simple yet effective method for distributing this type of information to people who don't have ready access to traditional management systems.

The use of centralized network management can pose several problems: processing and memory limitations, multiple remote consoles, a need to have software from the same vendor, a complex software package, and expensive software that requires special knowledge and skills [Ref. 6].

The addition of systems and applications management functions threatens to completely overwhelm today's enterprise management platforms, which have already proven to be deficient in handling network-specific data alone. The World Wide Web offers some useful features, including tools to address issues related to the management of systems and applications connected to the network, in addition to the traditional functions of network management. Using the World Wide Web can also help in addressing the limited availability and high skills needed for access throughout the enterprise, and support products from multiple vendors [Ref. 6].

Net management tools based on Web technology are just starting to be implemented by vendors. Some of the methods used by these tools include: [Ref. 6]

(1) Using the Web interface as a front-end to network management platforms. Data are stored in a familiar format, and are retrieved using the Web browser. The first generation of products use this technique to retrieve the data as a report, but none of them can report management information in real time. [Ref. 7]. This concept is illustrated in Figure 4-1:

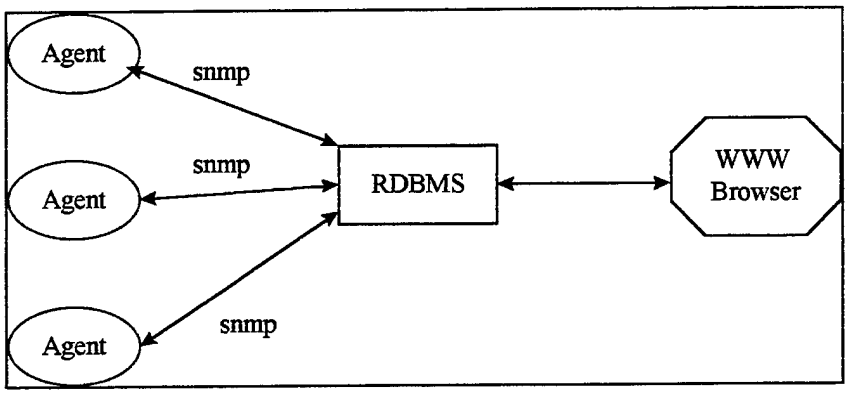

Figure 4-1. Web interface as a front end.

(2) Embedding Web-management capabilities in network elements, such as, hubs and routers. This method enables network managers to access the device from their browser as if they were accessing any other Web page so they can view the related management information [Ref. 7]. This method is illustrated in Figure 4-2:

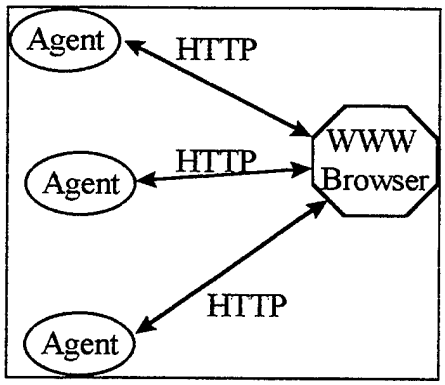

Figure 4-2. Web management capabilities in network elements.

(3) Using the Web as an interface, and getting the data from the SNMP based devices using SNMP commands. In this method, the information collected can be made directly available. This method does not require the use of network management platforms or embedding Web-management capabilities in network elements. This is illustrated in Figure 4-3:

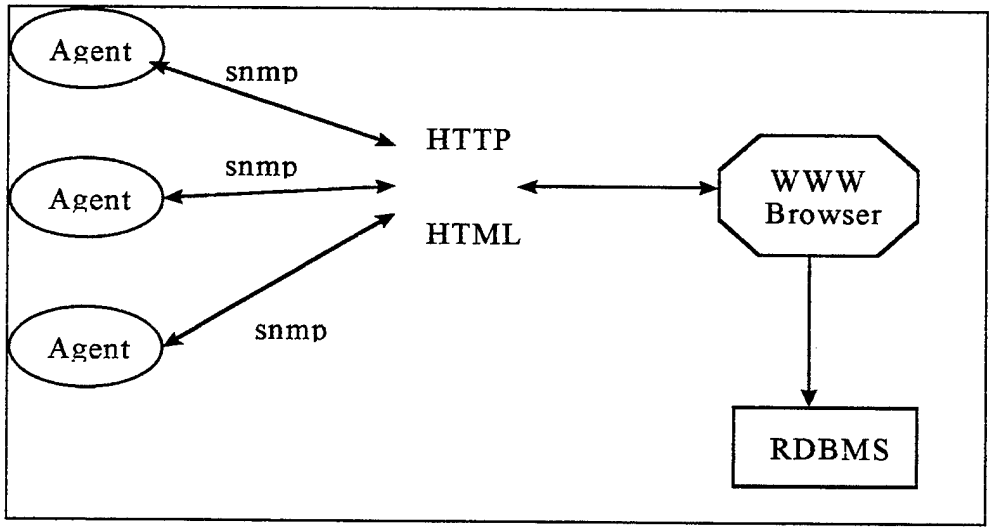

Figure 4-3. SNMP commands invoked using HTML/HTTP.

(4) The fourth method is similar to the third method, but the browser interface uses a Java applet as a tool to load, browse, and send requests for information using Java classes from SNMP based agents (Figure 4-4).

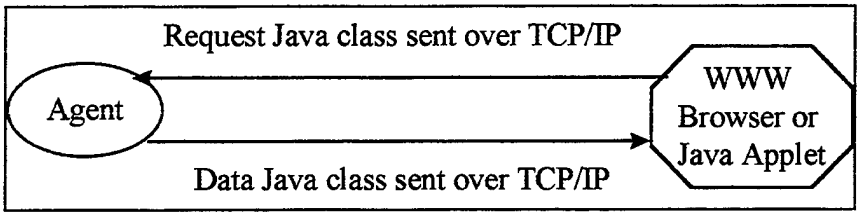

Figure 4-4. Using Java classes as "SNMP" packets.

2. Using HTTP and SNMP/CMIP for Network Management

In order to use the WWW infrastructure for network management, Hyper Text Transport Protocol (HTTP) is used as an interface layer between the devices that use SNMP. HTTP servers provide information that can be retrieved by WWW browsers. HTTP is a simple, stateless information retrieval protocol based on a TCP/IP suite. The retrieved information can be specified in several formats, such as, text, binary, MIME, and Hyper Text Markup Language (HTML). In order to manage current and future SNMP devices, some easy-to-implement changes to both SNMP and HTTP are suggested. These concepts are described below.

a. Changes in HTTP and SNMP-objects

This approach [Ref. 13] suggests a standardization for a mechanism for a Word Wide Web browser or network management application to have direct access to management information. The standardized TCP port for HTTP is port 80. A wide variety of information, including non-management related content, may be provided through this

port. A WWW browser or network management application should be able to determine where the management content resides on a HTTP server. In order to separate management information from a non-management related content for the browser, port 280 was proposed by the Hewlett Packard research group. This allows a browser or network management application to discover a HTTP server acting in a management role.

Two "HTTP manageable MIB" SNMP-based objects ("httpMgDefaultURL" and "httpMgSNMPEnabled") are proposed. These objects will allow a network management application using SNMP to query the "HTTP manageable MIB" to determine its HTTP management capabilities and interface. "httpMgDefaultURL" represents the complete URL for management access to the agent via HTTP. "httpMgSNMPEnabled" defines an agent's capability to perform SNMP over HTTP.

b. HTTP based SNMP

In order to manage network resources using HTTP it is necessary to have an application that speaks both HTTP and SNMP/CMIP. This approach [Ref. 14] can be achieved by extending standard HTTP servers, or by creating a proxy application that allows HTTP to be used for SNMP/CMIP requests. Mapping between SNMP/CMIP protocols and HTTP is defined such that SNMP and CMIP resources can be managed by using standard HTTP protocol. In one method, mapping is based on strings that can be handled by any programming and scripting language. A specified format of request/response for systems management using HTTP was proposed by the IBM network management group. This was done by defining a mapping between SNMP/CMIP and URLs (URL convention for SNMP/CMIP Management), and by specifying the format of

the information returned by HTTP. In a second method, the SNMP format of command was imbedded in HTTP so that it will invoke a Common Gateway Interface (CGI) program that will retrieve or change the desired information in the managed devices. Implementing it in a CGI technique offers a better performance than extending the standard HTTP servers. Both methods use HTML for basic network management and it very useful in situations where users are connected to the network using SLIP or PPP protocols. The assumption is that whenever it is necessary to provide a more sophisticated operations, they can be easily added using CGI or applets. [Ref. 22]

c. *Framework for Using HTTP and SNMP Management in the Web*

Bay Networks [Ref. 15], presents an architectural framework for delivering Web-based network management solutions. The framework features three distinct elements: The nearly universal Web browser; Web-enabled management applications; and HTTP-enabled devices. Figure 4-5 [Ref. 15], illustrates this framework:

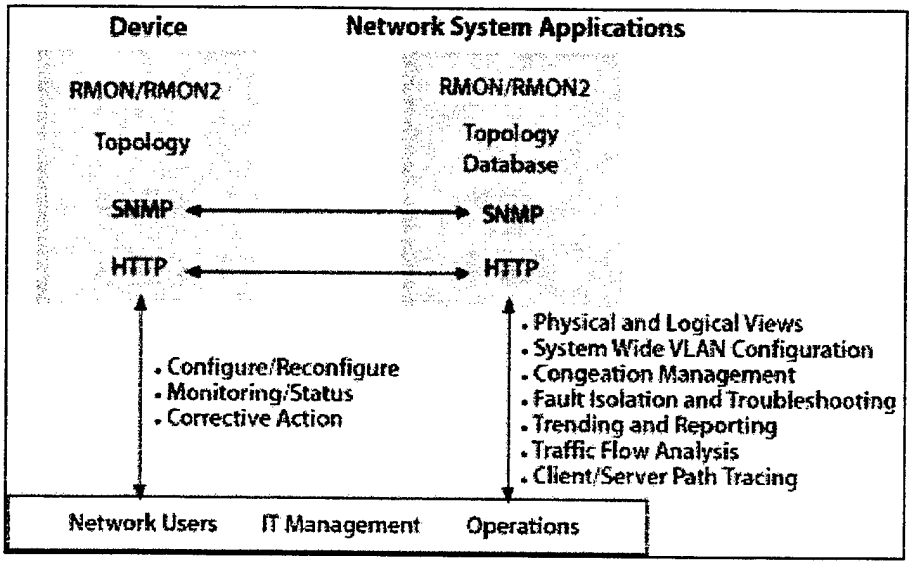

Figure 4-5. Bay Network Framework.

RMON/RMON2 data provides a detailed view of the characteristics of traffic flowing through the network, while multilayer topology information provides the management application with detailed knowledge of the physical and logical relationship between network devices. The multilayer topology capability is critical to managing a switched network, while RMON is critical to the monitoring and troubleshooting of client/server traffic. The main functions this approach supports are: correlation and presentation of network statistics, automatic baseline capabilities, and a single common point for launching all network management activities. With Web-based tools, the agent technology and network processing capabilities are distributed using HTTP protocol and Java.

Bay Networks [Ref. 16], offers an application that automatically discovers all network devices, as well as their physical and logical relationships. The product provides the ability to view and act on all devices of a certain type in one screen, rather than having to navigate across subnet views, as in typical network management systems.

Other Web-enabled applications provide access by staff to detailed information from any desktop, powerful network statistics viewing and integration tool that provides Java based tabulator and graphical output to show the state of devices and networks.

3. Web-based Network Management Using Java

The Java architecture of Sun Microsystems, which is gaining acceptance in the industry, has some attractive network management features. Java-based network management addresses some of the main drawbacks of SNMP/CMIP network management protocols, such as, communication overhead based on polling, a low level of security and portability between different architecture [Ref. 17], and the absence of communication between element management applications running on the same platform.

A proposed Java-based management system [Ref. 17], consists of a manager browser in the Network Management System (NMS), and an intelligent Java engine in the agent. The manager browser monitors and controls network elements in the network. The Java engine at a network element performs the management functions of an agent, and responds to the queries from NMS. The manager browser, as well as the agent, are stand-alone Java applications programs. The communication between the NMS and the agent is carried out by Java classes using TCP sockets. The implementation is based on collecting the user input, converting it to proper string format, and then using this string: a Java class containing the user input and agent name is created, compiled, and sent to the agent using TCP socket connection. At the agent, a background process that listens to the TCP port creates a worker thread to carry out the incoming requests.

Implementation of Java-based network management can be approached in two ways. The first is based on the Sun Microsystems Java operating system, *Kona*. In this approach, all the functions are implemented as part of the operating system core and, therefore, better performance is gained. The second approach is based on adding Java engine software along with the manufacturer's propriety operating system kernel. Table 1 compares the proposed system to current SNMP based system.

Characteristics	SNMP	Java/Web
Transport protocol	UDP	TCP
Daemon	SNMPd	Agent
MIB Type	ASN.1	ASN.1
Encoding	BER	bytecode
Message passing	SNMP PDU	Class
Extensible Agent	difficult	easy
Security	low level	good
Auto. Configuration	not defined	defined

Table 1. Java/SNMP comparison [Ref. 17].

SNMP uses UDP as a transport protocol, while a Java-based network uses TCP as the transport layer. UDP is usually sufficient for an environment where single IP datagrams are involved (e.g., campus area). However, it may not be sufficient in a WAN where remote management is essential. In that case, TCP should be used instead of UDP with the consideration of overhead cost. In SNMP the messages between the manager and the agents are in the form of SNMP PDU which compiles ASN.1 syntax and Basic Encoding Rules (BER). The Java system uses classes to communicate between the

manager and the agent. The Security feature of Java improves network management security.

Evaluation: Network management is by definition a distributed application. The proposed Java-based system addresses some of the major problems of current network management systems. These include portability across the platforms of different manufacturers, increased security aspects, and the need for a better GUI. It is possible to use Java for either GUI or for security and portability. The two options are independent. It is feasible to implement one or both of them. One of the major drawbacks in this system is that relaying on a TCP transport layer may increase overhead costs that were meant to be saved when SNMP is not used. Also, each query to the agent opens a new socket connection; therefore, compiling Java code and sending Java classes over the network might consume a lot of resources both from the network and the managed device.

4. Object Oriented, Web-based Enterprise Management

This proposal was initiated by BMC software, Cisco, Compaq, Intel, and Microsoft. The Web-based enterprise management (WBEM) proposal consists of three parts: [Ref. 18]

(1) An object-oriented model called HyperMedia Management Schema (HMMS), which is an extendable, object-oriented, data model that is used to model the managed environment.

(2) A communications protocol called Hypermedia Management Protocol (HMMP), an object-oriented management protocol implemented on top of HTTP.

(3) A Hypermedia Object manager (HMOM), a generic definition for management applications that aggregates management data and uses one or more protocols to present a uniform representation to the browser using HTML. The HMON could be implemented using existing development platforms as Java, Active X, CGI, CORBA, or COM.

The purpose of WBEM is to facilitate the use of the same terms and formatting in management applications, so that the applications can communicate, and users can more easily compare information from different applications and devices.

5. Merits, Demerits and more Discussion Points of Web-Based Network Management Tools

Before making the decision to implement a Web-based network management system in an organization, the merits and demerits of the concept, should be analyzed and some other issues, should be considered as well.

The main merits of Web-based network management are:

- The Portability problem is solved when using Web technology.
- Assuming pre-existence of a PC and a browser, hardware and software costs are marginal. All net managers need to gain access to the manager functionality is a standard PC running any browser.
- Remote access is simple. Net managers do not need to work from special consoles. Any dial-up connection will suffice.
- Management of platform expertise is optional. Web utilities present data in an easy-to-read way, and requires minimal training or learning skills.

- Information about the network status and configuration can be easily accessed by the organization workers and management; therefore reducing the number of calls to the help desk.

The main demerits of this concept are:

- Functionality is limited: Web utilities cannot match conventional platforms like SNMP for the depth of detail of management information.

- Real-time reporting is not yet an option.

- Security can be a problem. Unless the Web utilities are placed behind a firewall, they are subject to invasion by hackers.

Providers of commercial network management software have already began to market Web-based tools for the main components of their systems. It is a paradigm shift from a tools-based approach to a process-based one. Yet these tools have some limitations that should be considered:

- Sun Microsystems, Inc. has proposed a series of Java Management Application Interfaces (JMAPIs). JMAPI is a set of interfaces that read and write Java objects, such as status information, directly into a relational database for management. The API uses a remote method invocation as its remote communication mechanism. Users will be able to use different pieces of an application together. JMAPI allows a high degree of integration so that the user is able to navigate seamlessly from diagnosing a router problem to a help-desk problem [Ref.19].

- Building, maintaining, and controlling Web management applications might not be a simple mission. "25-30% percent of large sites that have attempted to cobble together Web-based management from existing platforms and tools failed". [Ref. 20]

- Does Web-based management herald the end of SNMP? Java applets can be activated from any browser, and can detect key information and transmit it to a database, a management application, or a Web browser. Some claim that SNMP is still the bedrock of enterprise management. For example, the management console will act as a proxy agent, collecting data from all the legacy SNMP agents on the network. The data then will be posted to an SQL server and retrieved by applications running on the Web server.[Ref. 20]

- Security threat: On the one hand, many vendors agree that the security issues with browser-based management are no worse than with traditional approaches; on the other hand, some claim that the security issue is a big worry. The Internet is known as an insecure net. While Java offers several built-in security mechanisms, some must be bypassed in order to perform management tasks. For example, applets are not allowed to read or write files on a client's hard disk. But if Java applets are to be used for software distribution, that restriction must be circumvented. Similarly, applets can't set up any network connection except to the server from which they came. Net managers could open separate browser sessions for each device on the network

they need to monitor. But if they need to keep tabs on hundreds or thousands of components, this approach is impractical [Ref. 20].

- Performance: Running management apps on a Web server also raises some serious performance issues. The fundamental problem is the agonizing delays present on the Internet itself. Further, processing SNMP polls can be CPU-and bandwidth-intensive, which can slow response time even more. And, on top of that, it takes about 90 seconds to transform SNMP data into HTML pages, introducing further lag time. Net managers accustomed to the real-time feedback they get with proprietary platforms are in for a disappointment. [Ref. 20]

V. PROTOTYPE DESCRIPTION

A. PURPOSE AND SCOPE

The goal of building the prototype are as follows: The first is to show a proof-of-concept system, which uses the Web as a tool for managing System Management department labs. The prototype structure provides the ability to access and control the information related to the labs from any Internet browser, by the main user and by other users, such as students and faculty (given that the user has the appropriate permissions). Second, the system can be embedded later in the department intranet, and provide both the students and the faculty access to the labs information. Third, it served as a test bed for the relatively new technology of database remote access using the Web infrastructure.

In order to keep the scope of the prototype close to the user needs (described later in this chapter), the prototype is focused on providing an application for managing the labs configuration. That includes host configuration (software and hardware), labs diagrams and other device details.

B. ASSUMPTIONS

Due to the nature of the life cycle of IT equipment, the courses taught, and research areas, the lab configuration is changed frequently. This includes upgrading current equipment, installing new PCs, printers, servers and other peripheral equipment, as well as upgrading and installing new software and operating systems. Maintaining, operating and changing the lab configuration requires a way to manage the information so

that it will serve the lab Manager, as well as faculty, and students of System Management department labs. Some assumptions were considered when building the prototype:

- The fact that the system would not be used frequently, and the need to avoid the training requirements for the different users, are the main factors considered regarding the user interface design. The goal is to keep the user interface simple as possible.

- Web technology should be used in order to provide the different users with the ability to access lab configuration data from different locations using an Internet browser.

- The application uses the services of a Web server. Assuming that the System Management (SM) department would have an intranet in the near future, the proposed application would be one of the services provided by the department intranet. Therefore, this application does not require a dedicated server.

- Using SQL RDBMS (such as MS-Access) provides the option of building simple ad hoc queries and reports that are not readily available.

- The proposed application should address the natural transition problems from a paper environment to a Web management environment by providing the ability to print reports and query results easily.

C. DESCRIPTION OF USER NEEDS

The main users of the system are the lab staff of the SM department. They manage the lab configuration and handle the labs maintenance, which includes installing new hosts, upgrading current hosts, installing software according to user requests, maintaining the Token Ring network configuration (servers, hubs MAUs, maintaining the printers), and serving other user requests. In order to keep track of the lab configuration, the user should be supported with a tool that has several basic functions to support the configuration management tasks. The following list represents the users needs:

- The ability to retrieve and update information about the lab hardware which includes hosts, servers, printers, and network components.
- The ability to retrieve and update information about the lab software.
- The ability to acquire a broad view of the lab diagrams, as well as get detailed information about a specific lab diagram.
- The ability to support routine administrative tasks, such as managing user accounts, and installing new software and hardware.
- The ability to learn user interface easily.
- The ability to search for a particular device.
- The ability to run queries and reports about the lab configuration data (e.g., IP-addresses, serial numbers, physical locations, and free slots).

D. DEVELOPMENT TOOLS

WebSite and Cold Fusion as a database application development tool have been used as the main tools in building the prototype. The following is a short description of the tools that have been used in developing the prototype:

- **WebSite** is a Web-server software tool that supports the publishing of Web pages on the Internet or an internal intranet. WebSite offers a wide range of programming options using Common Gateway Interface (CGI) to interact with different programming environments. It also supports the Application Programming Interface (API) technique for better performance.

- **Cold Fusion** is a Web-application development tool with the capability of using the Web to create dynamic-page applications and interactive Web sites. Cold Fusion provides a way to quickly build powerful Web applications that integrate with key server technologies such as relational databases. Its main advantage is that it provides a template for developing HTML forms without the need to write any CGI programs. Instead, applications are created by combining standard HTML files with Cold Fusion Markup Language (CFML) tags. Cold Fusion 2.0 uses Netscape's server API (NSAPI), Microsoft's server API (ISAPI), and WebSite's API (WSAPI) to connect directly to the major Web servers supporting these standards. Cold Fusion also supports the CGI technique to communicate with other Web servers. It works with a wide variety of Web servers running under Windows NT/95. [Ref. 21]

- **Microsoft Access database** is used in the server for the labs data. The access to the database through the Web is achieved using Cold Fusion as an interface between HTTP and DBMS, based on ODBC (Open Database Connectivity).

- **HTML** is Hyper Text Markup Language, which is used for building Web-based pages.

E. DEVELOPMENT PROCESS

The development process includes the following steps:

- Conducting interviews with the users to study their environment and main problems in managing the labs configuration.

- Analyzing the users' needs, and proposing the main functions and scope of the prototype to the labs administrator as the main user.

- Learning some development tools (e.g., Java, CGI, Cold-Fusion, and Web-site) while searching for current Web-management tools.

- Presenting the user with a conceptual design of the prototype.

- Building the prototype while getting continuous feedback from the user.

- Presenting the prototype to the labs director.

F. APPLICATION DESCRIPTION

The following describes the main functions, which are implemented in the prototype followed by some screen shots. One of the advantages of using a Web-browser

is the printing capability. Throughout all the screens the user can print the information retrieved from the database by using his browser "print" button. In that way every query displayed can be used as a report.

The first screen is the login screen where a user is requested to input his login and password. The system has some processes of security to prevent unauthorized users from accessing the data; For example, the permissions given to a regular user and the system administrator are different. Running in a browser environment, the application has a security process to prevent a user from accessing internal Web pages of the application without first providing a login and a password. A more detailed description of the security concept implemented in the prototype is given in the developer manual (Appendix A). The following figures describe the main screens a user or an administrator will see while working with the application. A more detailed description of the prototype functions and features are given in the USER MANUAL (Appendix B).

Figure 5-1 shows an attempt to access the main system Web-page without first providing a login name and password in the login screen.

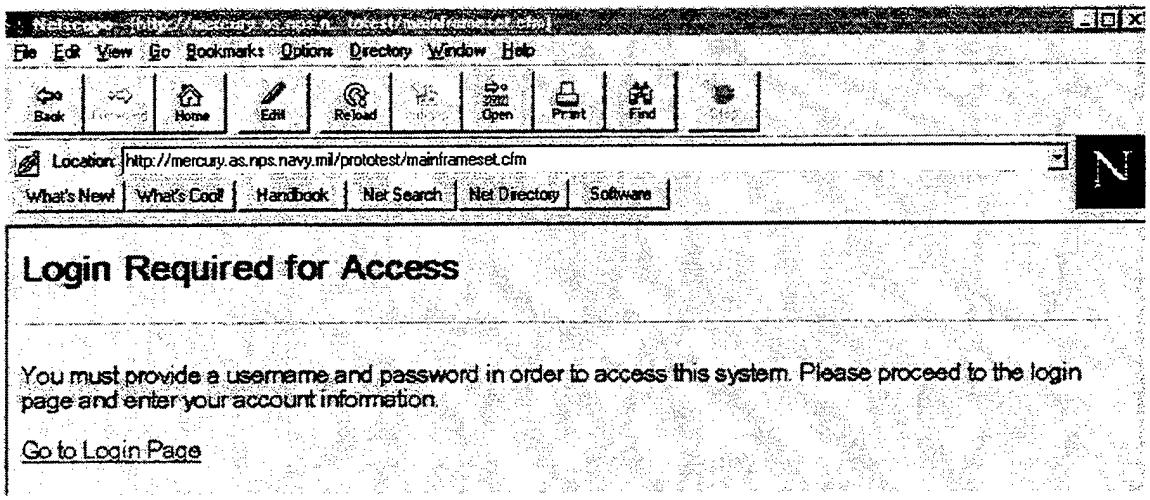

Figure 5-1. Response to incorrect access.

Once the user is logged in, the main screen of the application is displayed as shown in Figure 5-2.

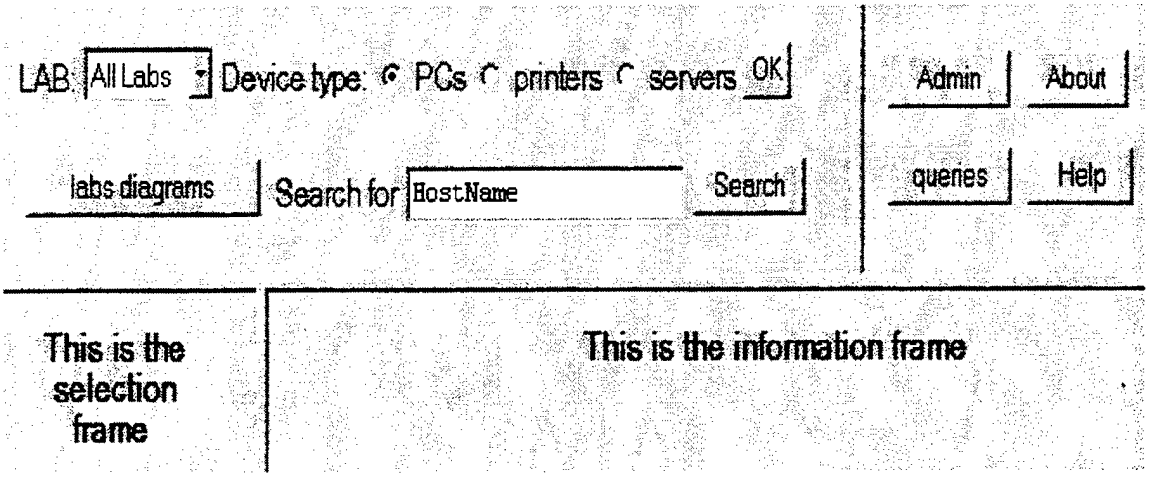

Figure 5-2. Main screen.

The main screen has four frames. The upper left frame is where the user checks the type of information he needs, that is, the lab (the default is all the labs) or the type of device (e.g., PCs or printers servers). The user can also choose to display a lab diagram or

the lower left frame guides him with the options that can be currently invoked. For example, if the user chooses the PCs in LAB-151, a list of the current hosts in that lab would be shown in the lower left frame (as shown in Figure 5-3). The user should select the correct PC to display, and the function to invoke (view, update or delete) according to the permissions that were given. The information retrieved about the selected device is displayed in the lower right frame (as shown in Figure 5-3).

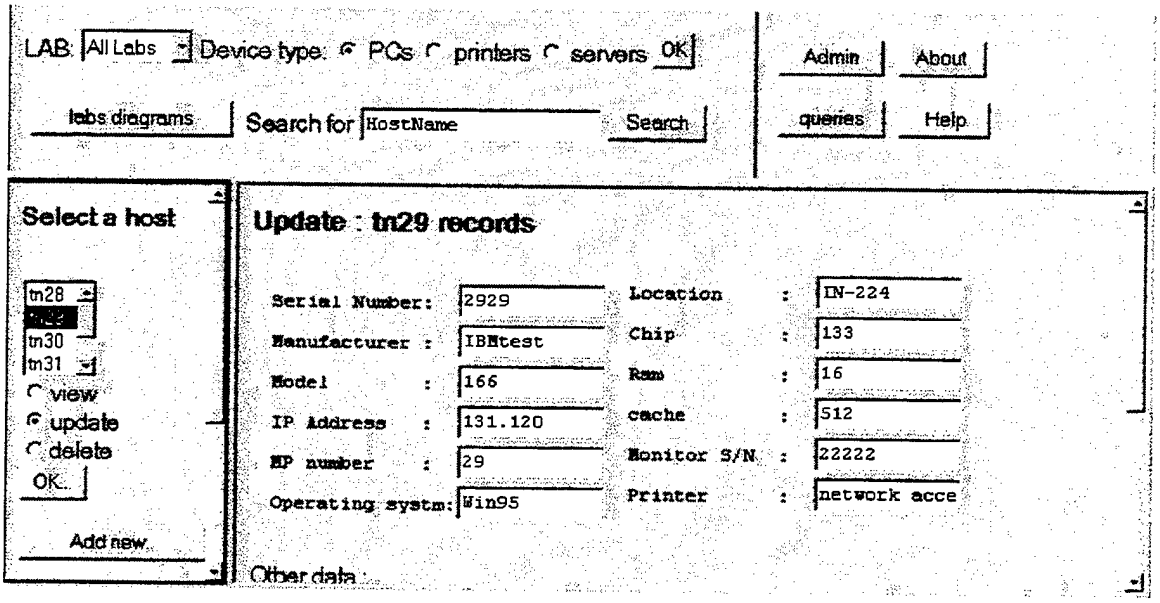

Figure 5-3. Updating host details.

More information about the system can be retrieved by scrolling down in the lower right frame and selecting other relevant buttons to get detailed information about the system. This is demonstrated in Figure 5-4.

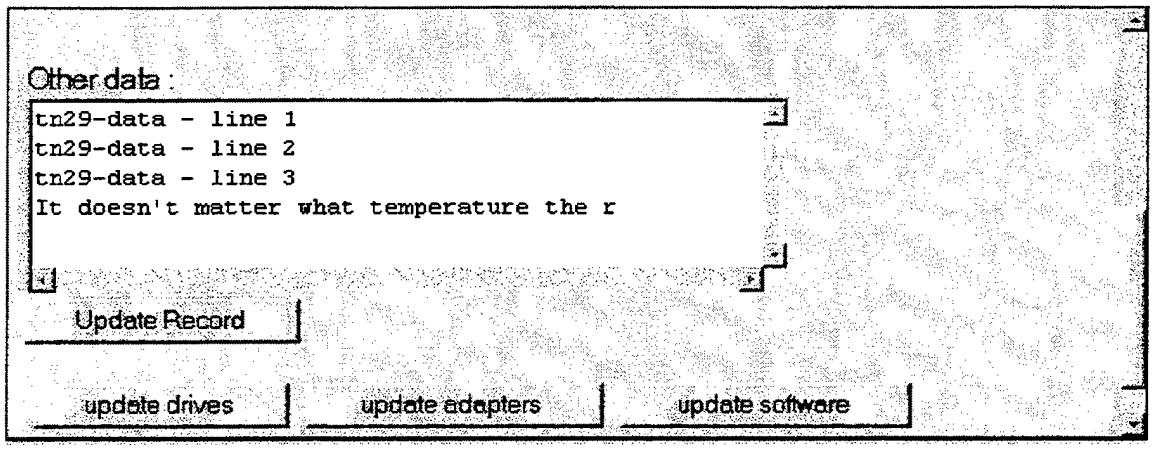

Figure 5-4. Getting more system data.

Queries and admin function buttons are in the upper right frame. When requesting queries, the available queries list is shown in the lower left frame. The results of a selected query are shown in the lower right frame as shown in Figure 5-5.

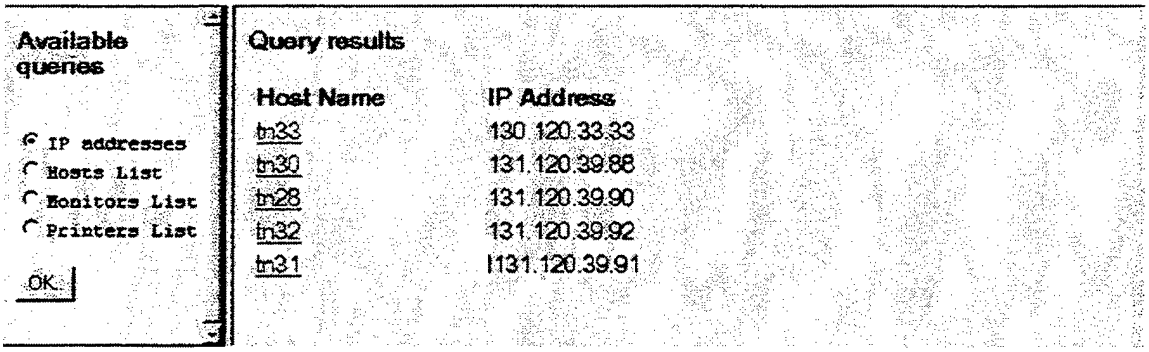

Figure 5-5. Query results.

The Admin function provides the ability to manage users (only for an authorized user). Figure 5-6 shows the screen a user would get when pushing the admin button and asking to change his own password.

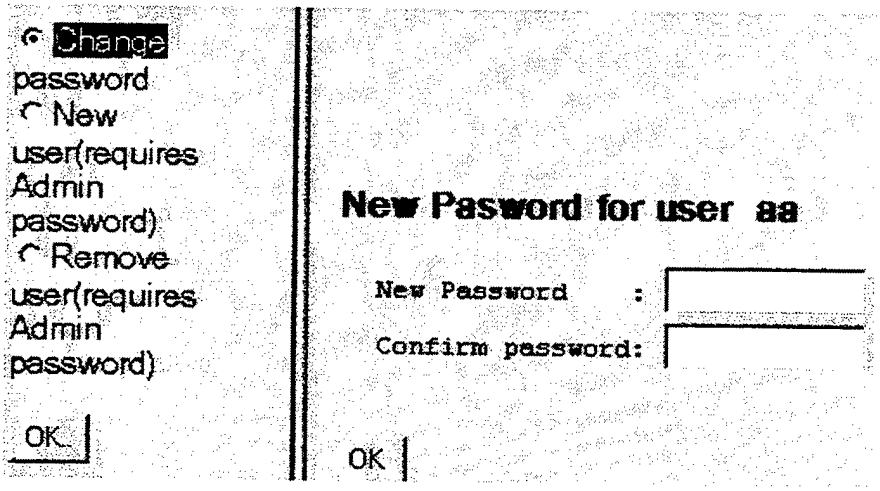

Figure 5-6. Admin button - changing password.

An administrator has the permission to add new users, or remove current users from the system.

VI. CONCLUSIONS AND FUTURE RESEARCH

A. SUMMARY AND CONCLUSIONS

Networks are vital to the success of today's organizations, for both internal and external activities. The complexity and the cost of current network management tools on the one hand, and the Internet technologies such as, World Wide Web and Java language on the other hand, have motivated the research and development of new Web-based technologies to support network management systems. The World Wide Web has emerged as a new paradigm in information access and display, becoming the preferred method for accessing corporate data over the enterprise network. Today most of the vendors of network management systems are basing their next generation tools on Web-based management [Ref. 20]. Web-based management is a paradigm shift from a centralized management concept to a distributed management-data concept. Web technologies can serve as an excellent infrastructure for simple and powerful tools to address the current problems of network management systems. Web-based tools can provide portability across platforms, and a good framework for network management application architecture. Using Web technologies have more benefits, such as easy-to-reach information, consistency in presenting and accessing information and objects, and operations reuse.

Most of the current network management tools are based on SNMP. Therefore, new methods and solutions should address the issues of compatibility with existing infrastructure, and the ability to integrate with the existing network manager. Web-based

solutions do have some limitations, the major one being the security issue. Web-management tools can be set up to be accessed from anywhere on the Internet, and the user can define his station as a management station. Current security tools, such as password and firewalls, are not sufficient to avoid the risk of Internet hackers. However, Web-based management tools will play a major role in providing the future network management tools and solutions. The effort to provide Web-based enterprise management specifications by industry leaders is a good sign of this paradigm shift.

B. SUGGESTIONS FOR FUTURE RESEARCH

This thesis covered most of the new methods that have been proposed today by different vendors and research groups for Web-based network management solutions. On the other hand, using web-based tools, the prototype has implemented (based on the user needs and the thesis scope) the configuration management part of the network management model. In order to extend the prototype and the research, the author suggests implementing some other network management functions using SNMP, Java, or HTTP (or any combination of them). For example, using HTTP and SNMP the system can provide the user the ability to query the network devices and automatically update the configuration database. Another example is building a Java applets for both the server and the clients, such that the configuration data (or any other desired data) can be transferred as Java classes between the clients and the server.

The IETF attempts to define a new version of SNMP in order to address the current limitations of SNMP; for example will the new standard will address web-based proposals.

Several providers of network management solutions (e.g., Hewlett-Packard, Bay-Networks, 3Com, and Cisco) intend to launch new products and versions of network management systems and tools through the second half of 1997. Future research should evaluate these solutions, in particular the way they integrate the Web technology.

Future research can also be done in the field of hypermedia tools for network management systems. Although incorporating hypermedia implies an increase in resources and assets needed for network management, some network management functions can benefit from this technology. Such research should address ways to evaluate hypermedia functions and capabilities; for example, whether a hypermedia system be open or closed.

The author suggests paying attention to the market processes before doing any future research. In the near future the main network management solutions providers are likely to publish research papers about the new Web-based products.

The security limitations of the Web technology imply that it does not necessarily fit a military environment. Future research should first determine whether more secure tools are feasible, and then analyze the cost effective of a transition from current tools.

APPENDIX A. DEVELOPER MANUAL

A. CONCEPTS OF DEVELOPMENT TECHNIQUES

1. User Interface

The main concept behind building the prototype interface is to let the user work in front of one main screen. As described in the user manual (Appendix B), the user can get most of the information on the main screen with no need to remember a list or tree of screens. In order to achieve this, HTML frames have been used. Using frames also keeps menu areas stable. Only the area of displayed information resulting from a user's query is changed. Using this technique it is very simple for a user to be familiar with the application in order to get the required information (according to his level of permissions).

2. Security

Security is implemented in the prototype in two ways. First, by using Cold Fusion cookies technique, only authorized users can access the system; in particular, only the system administrator can modify the configuration database. Cookies are a general mechanism for storing and retrieving information about the client (browser). The cookies mechanism can be used to store persistent client variables in the system registry on the Web server. These variables are specific to an individual browser accessing the Cold Fusion application. Using this mechanism, the system also prevents any attempt to access its pages without first providing a login name and a password. Second, in the appropriate screens, some functions are disabled for non-authorized users.

3. Database Access Through A Browser

In order to retrieve and display data from a database, a Cold Fusion template that includes both CFML and HTML is created. The template contains two main sections; In the first one (which is usually CFML code), the query is built and processed. In the second one the query results (which may be dynamic) are used (within the HTML code) for output or as parameters for other forms and pages. The database query is implemented using Structures Query Language (SQL) within a special Cold Fusion CFML tag. Accessing the database requires an ODBC link, which is defined prior to building the HTML/CFML code.

B. DATABASE STRUCTURE

The main entity in the database is the device type (e.g., host, hub, or printer). For each device type there are several tables that represent the device attributes. The tables have the same unique key, which identifies the same device entry over the different tables. A table may hold a relationship(s) field, which is a "pointer" to a different device type. For example, the tables relationships shown in Figure A-1 represent the attributes to be stored for the lab PCs.

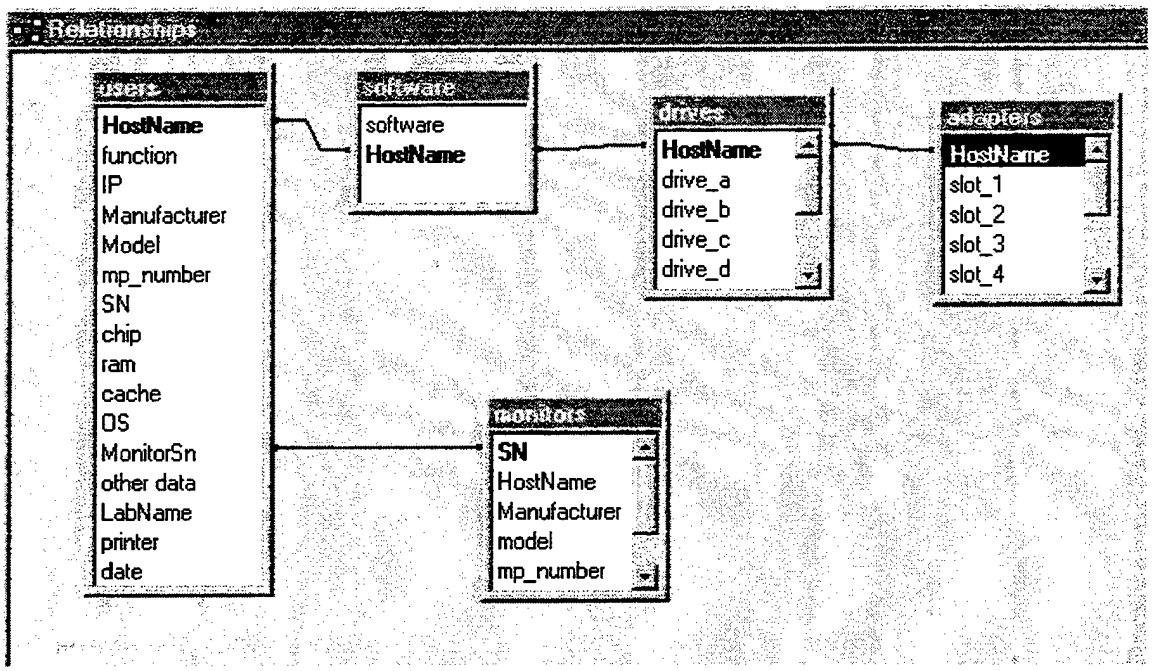

Figure A-1. Hosts tables Relationships.

With the structure and relationships shown above, it is simple to build input forms, as well as retrieve the data for different queries and forms.

In order to manage the authorized users and their permissions, a second database is handled. This database is accessed only by the templates that handle the login procedure (cookies mechanism).

C. COLD FUSION

In a normal Web site, pages are simple text documents marked with HTML. These pages are sent out to the user's browser by the Web server as they are requested. A Cold Fusion web application begins with a collection of dynamic-page templates instead of static HTML documents. A template is simply a text file that contains both HTML and the Cold Fusion Markup Language (CFML). Instead of being sent directly to the user's browser, templates are pre-processed by the Cold Fusion application server, which generates an HTML page, and is then sent to the user's browser.

Figure A-2 below shows what happens when a Web browser requests a Cold Fusion page.

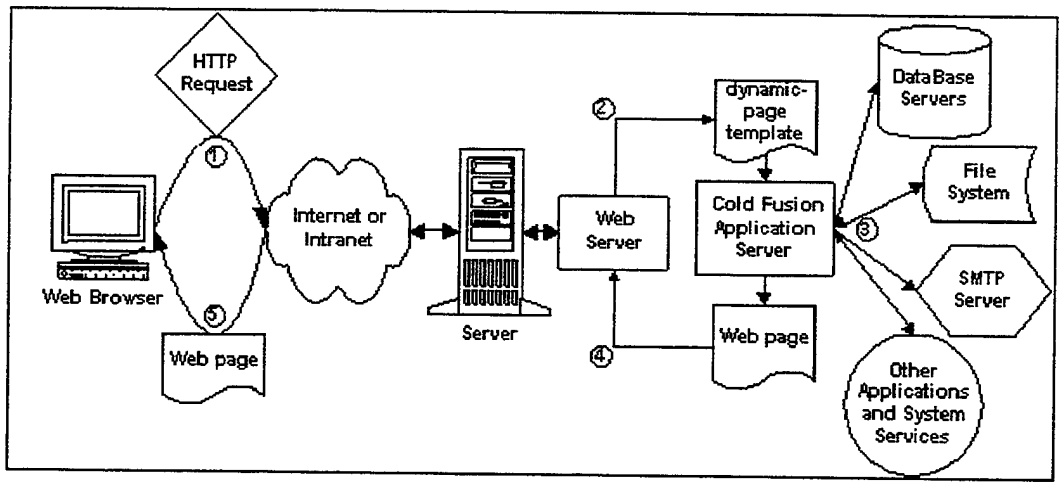

Figure A-2. Cold Fusion Page Architecture [Ref. 21].

When a user clicks a "Submit" button on a form or a hypertext link, the user's Web browser sends an HTTP request to the Web server via the Internet or an intranet. The Web server passes the data submitted by the client and the appropriate template file to the Cold Fusion application server, either through a server API or CGI. Cold Fusion reads the data from the client, and processes CFML commands used in the template. Based on the CFML commands, the application server interacts with database servers using ODBC.

Cold Fusion dynamically generates an HTML page and returns it to the Web server. The Web server then passes the page back to the user's Web browser. The difference between a normal page and a dynamic page is that, in a dynamic page, the template is pre-processed by Cold Fusion, and it contains commands in addition to HTML.

The Cold Fusion application server runs as a multi-thread system service and handles complicated processing. The application server communicates with the Web

server either through a CGI or through a native Web server API. The native web server APIs offers additional features and significantly increased performance. Instead of launching a CGI executable, servers supporting an API communicate directly with the Cold Fusion application throughout a DLL. [Ref. 21]

D. MAIN PROCESSES

Figure A-3 describes the main processes of the prototype. This diagram and Table A-1, may be very useful in understanding the application files structure, and relationships with the application functions. It is necessary for someone who intends to work with and make changes to this prototype.

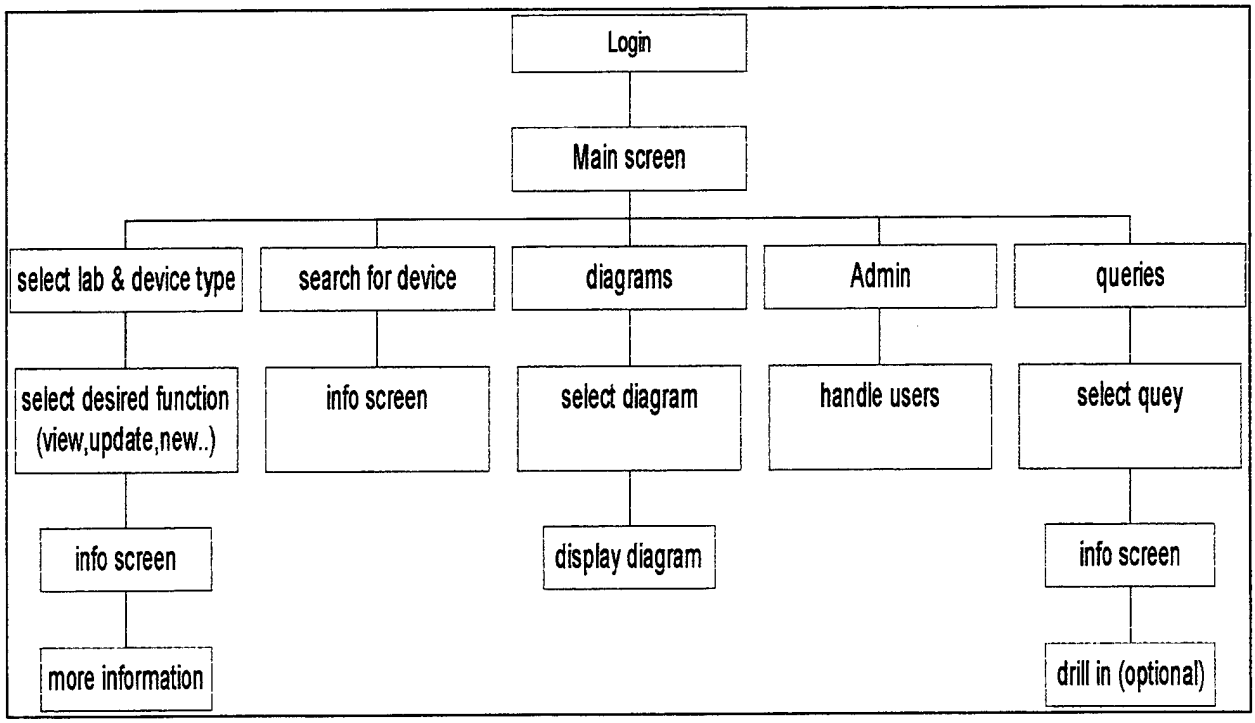

Figure A-3. Main processes of the prototype.

E. MAIN PROCESSES AND FILES INVOLVED

Table A-1 describes the main functions implemented in the prototype with the correlated involved files and methods that were used.

Function/process	Files involved	Methods used
login	main.htm, secure.htm	Cold Fusion query, cookies
main screen	mainframeset.htm	HTML frames CFINCLUDE
upper left frame (selecting lab, asking for lab diagram, search request)	queryframe.htm	HTML forms and input methods
lower left frame	device_query.cfm	Using Cold Fusion for Dynamic dialog box
upper right frame	moreinfo.htm, about.htm help.htm	HTML forms
lower right frame	infoframe.htm	
administrating users	admin.cfm, adminfunctions.cfm, updatepassword.cfm, newuser.cfm, deleteuser.cfm	CFINSERT CFUPDATE
show diagram	selection-diagram.cfm, diagram-to-htm.cfm	GIF files
queries	get_query.cfm	Cold Fusion query, dynamic URL results
view/update/new a device	view.cfm, update.cfm, new.cfm, insert.cfm	
view device attributes	drives.cfm, adaptres.cfm, Monitor.cfm, software.cfm	
update device attribute	update_and_return,cfm, update-drives.cfm, update-adapters.cfm, update-software.cfm	

Table A-1. Main Functions Implemented in the Prototype.

APPENDIX B. USER MANUAL

A. GETTING STARTED

To get started, move to http:/mercury.as.navy.mil/prototest/main.htm[1] which brings up the user authentication screen. Basically, there are two options to login: as a regular user or as an administrator. The administrator has the ability to manage users and to modify the database data. Other users can only view or invoke queries about the data.

After successfully logging in, the main working screen appears. This screen is divided into four areas (frames).[2] The upper two frames are static frames for selecting the type of information to display (e.g., lab, device type, diagrams, or queries). The lower left frame contains a dynamic selection list, which corresponds to the selection in the upper frames. This frame offers the selection of the specific device, query, or lab-diagram, which is displayed in the lower right frame. The main screen is intentionally built so that an infrequent user does not have to be familiar with many different screens in order to be able to retrieve or update data. Most of the work is done with one main screen. The rest of this appendix describes how to perform the different functions of the application.

---

[1] This URL may be changed according to the server allocated for the system, and should be checked by the lab's administrator.

[2] Some screen shots of the application are given in Chapter V of this thesis as part of the application description.

B. RETRIEVING INFORMATION

1. Through Device Type And Location

In the upper left frame, select the lab name (the default is all the labs), and the device type you are looking for (e.g., PC, server, or printer). Click the "OK" button for the list of matched devices of the required lab. The device list is displayed in the lower left frame as a selection list. Select the device, and click the "OK" button. The retrieved information is displayed in the lower right frame. In order to get more details about the same device, scroll down in the data frame, and click the relevant button for more details (in the same frame). The browser can always be used to go to the previous screen, or to print the displayed data.

2. Searching For A Device Name And Retrieving Its Details

This is a convenient way to directly retrieve data about a specific device using the device name. In order to do so, enter the device name in the search area of the upper left frame, and click the search button. The device details are displayed in the lower right frame.

3. Displaying Labs Diagrams

Choose the "labs diagrams" button in the upper left frame. The list of available diagrams are displayed as a selection list in the lower left frame. Select the desired diagram. The diagram is displayed on the whole screen. Press the "back" button in your browser to return to the main screen.

4. Queries

Clicking on the queries button in the upper right frame, results in the list of available queries (e.g., Hosts-list or IP-addresses) in the lower left frame. To obtain the query results select the required query from the list, and click "OK". The query results are displayed in a hyperlink format. This means that by pressing a highlighted result you can get the device details. In order to return to the query results data, either click on the browser "back" button or invoke the query again.

C. UPDATING DATA

This function can only be accessed by the administrator. After selecting the device type and location as described in section B-1, an administrator may choose to update the device details. First, the specific device name should be selected from the device list in the lower left frame. Then, by checking the "update" radio button and clicking "OK", the device details appear in a "Form" format in the lower right frame. An administrator may update the device details by clicking the "update" button. Then, by scrolling down the frame and selecting the relevant button, an administrator can update other device details.

D. DELETING A DEVICE FROM THE DATABASE

This function is can only be accessed by the administrator. After selecting the device type and location as described in section B-1, an administrator may choose to delete the device records. First, the specific device name should be selected from the device list in the lower left frame. Then by checking the "delete" radio button and clicking "OK", the system confirms the delete operation request. The administrator is notified when the device records are removed.

E. ADDING A NEW HOST

This function can only be accessed by the administrator. After selecting the device type and location as described in section B-1, an administrator may choose to add a new device by selecting "add new device" in the lower left frame. The device field appears in a "Form" format in the lower right frame for data input. Then, by scrolling down the frame and selecting the relevant button, an administrator can enter other device details.

F. ADMINISTRATING USERS

1. Changing User's Password

Any user can change his password through the system. To do so, click the "admin" button in the upper right frame, select the "change password" option (default) in the lower left frame, and click "OK". A guided form for changing your password will appear in the lower right frame.

2. Adding And Removing Users

These functions can only be accessed by the system administrator. To add a new user to the system, choose the "admin" button from the upper right frame, select the "add new user" in the lower left frame, enter the new user login name and password, and submit the data.

In order to remove a user from the system choose the "admin" button from the upper right frame, select "delete a user", and select the user name from the list in the lower left frame. The system confirms the action before removing the user.

LIST OF REFERENCES

1. Stallings W., *Data and Computer Communications*, fourth edition, Prentice Hall, 1994.

2. Leinwand A., Fang K., *Network Management A Practical Perspective*, Addison Wesley, 1993.

3. Stallings W., "Patching the Cracks in SNMP," *BYTE*, August, 1996, pp. 55-56.

4. University of Michigan, Information Technology Division, http://smurfland.cit.buffalo.edu/NetMan/ProdRevs/UnivMichReport.html

5. Wilson T., "See the big picture," *BYTE*, October, 1996, pp. 107-112.

6. Sridhar S., "Managing Enterprise Networks Using The World Wide Web," Naval PostGraduate School, September 11, 1996.

7. Larsen A.K., "The next Web Wave: Network Management," *Data Communication*, January, 1996, pp. 31-36.

8. HQ AETC (Air Education and Training Command) NMS Evaluation Documents, http://www.aetc.af.mil/AETC-NetMgmt/nms-menu.html

9. Bay Networks, "Web-Based Network Management: Linking to the future of Network Management", http://www.baynetworks.com/Products/Papers/webbased.html

10. Fitzgerald J., *Business Data Communications: Basic Concepts, Security, And Design*, John Wiley & Sons, Inc., 1993.

11. Stallings W., *Network And Internetwork Security*, Prentice Hall, 1995.

12. Bieber M., Vitali F., "Toward Support for Hypermedia on the Word Wide Web", *Computer*, Jan, 1997, pp62- 70.

13. Harrison Brian(HP), Mellquist Peter E.(HP), Pell Adrian (HP),"Web based system and Network Management" - Internet draft, ftp://ds.internic.net/internet-drafts/draft-mellquist-web-sys-01.txt

14. Deri L., IBM Zurich Research Lab, "IBM - HTTP-based SNMP and CMIP Network management" - Internet draft, http://www.zurich.ibm.com/~lde/draft-deri-http-mgmt-00.txt

15. Bay Network white paper, "Web based network management" http://www.baynetwroks.com/Products/Papers/webebased.html

16. "Bay Networks Announces Web-Based Network Management", http://www.baynetworks.com/News/Press/9609171.html

17. Gottfried L., Hosson Ku, Baranitharan S. and Anand N., Arizona State University, "Network management agents supported by JAVA Environment".

18. BMC software, Cisco, Compaq, Intel, and Microsoft, "Web-based Enterprise Management proposal", July 16, 1996, http://wbem.freerange.com

19. T.Corcoran C.T., "Managing Network ills Network managers tackle management-tools deficiencies with Web technologies", http://www.inforworld.com/cgi-bin/display/Archives.pl?dt_iwe42-96-82.htm

20. Jander M., "Welcome to the Revolution", Data Communications, Nov. 21, http://www.data.com/round.sups/monitor.html

21. Allaire Corp., *Cold Fusion User Guide*, http://www.allaire.com

22. Barillaud F., Deri L., and Feridun M., "Network Management using Internet Technologies", http://www/zurich.ibm.com/~lde/M97/lM_Paper.html

I. INITIAL DISTRIBUTION LIST

1. Defense technical Information Center.....2
   8725 John J. Kingman Road., Ste 0944
   Ft. Belvoir, VA 22060-6218

2. Dudely Knox Library.....2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5101

3. Dr. Suresh Sridhar, Code SM/Sr.....1
   Naval Postgraduate School
   Monterey, CA 93943-5105

4. Rex Buddenberg, Code SM/Bu.....1
   Naval Postgraduate School
   Monterey, CA 93943-5105

5. Dr. Norman Schneidewind, Code SM/Ss.....1
   Naval Postgraduate School
   Monterey, CA 93943-5105

6. Leon Sahlman, ...1
   System Management Department
   Naval Postgraduate School
   Monterey, CA 93943-5105